ESG Lab Spotlight

Bitglass Cloud Access Security Broker

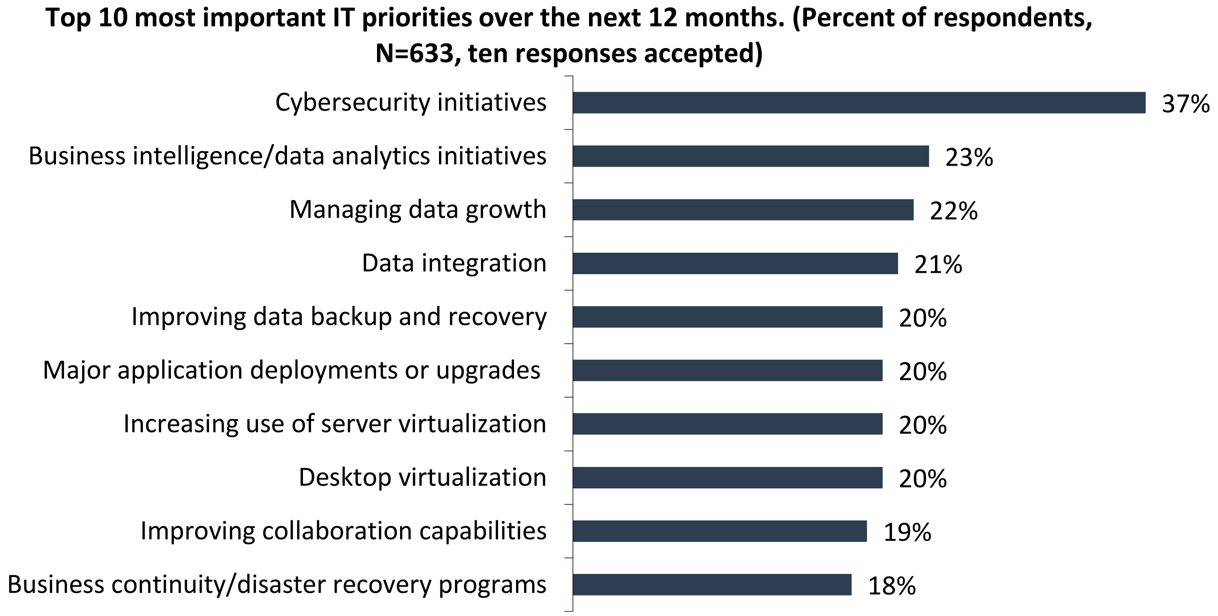
Date: February 2016 **Author:** Tony Palmer, Senior Lab Analyst

Abstract: *This ESG Lab Spotlight examines how the Bitglass Cloud Access Security Broker (CASB) provides access control, data loss prevention, and threat detection for data that has moved outside the firewall via public cloud applications and bring your own device (BYOD) policies.*

The Challenges

ESG recently asked a sampling of IT professionals and managers to identify their top IT priorities, and 37% of respondents noted cybersecurity initiatives as one of the highest IT priorities within their organizations in 2016 (see Figure 1).[1] In the same survey, 75% of organizations indicated that they currently use public cloud services for a wide variety of applications, with 19% planning to use the public cloud in the near future. Respondents also stated that providing employees with mobile devices and applications is one of the initiatives driving the most technology spending at their organization over the next year, while 20% identified interaction with customers on their mobile devices.

Figure 1. Top Ten Most Important IT Priorities



Source: Enterprise Strategy Group, 2016.

In a world of cloud-based applications and mobile devices, IT must secure data that resides on cloud providers' servers and is accessed across the internet from employee-owned devices, whether desktop, laptop, or mobile—managed or unmanaged. Existing security technologies are not well suited to solving this challenge, since they were developed to secure data that resides on company-owned resources within the corporate network perimeter.

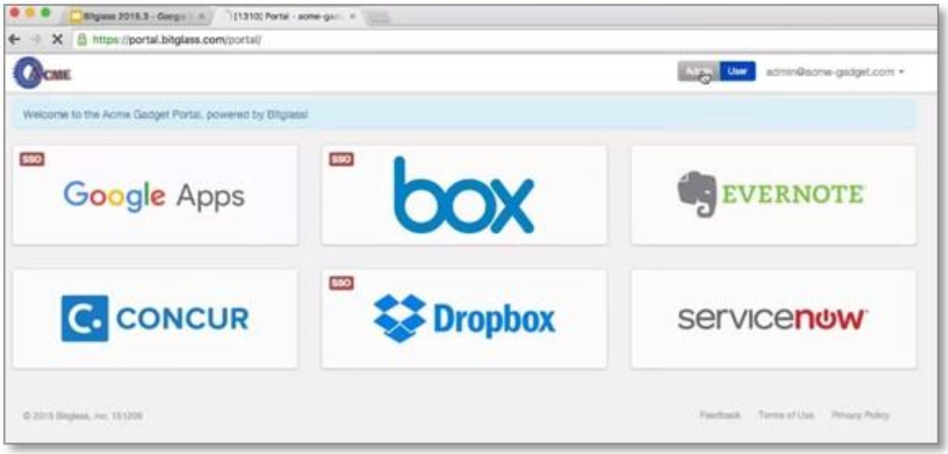
[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, to be published.

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments. This ESG Lab report was sponsored by Bitglass.

Bitglass

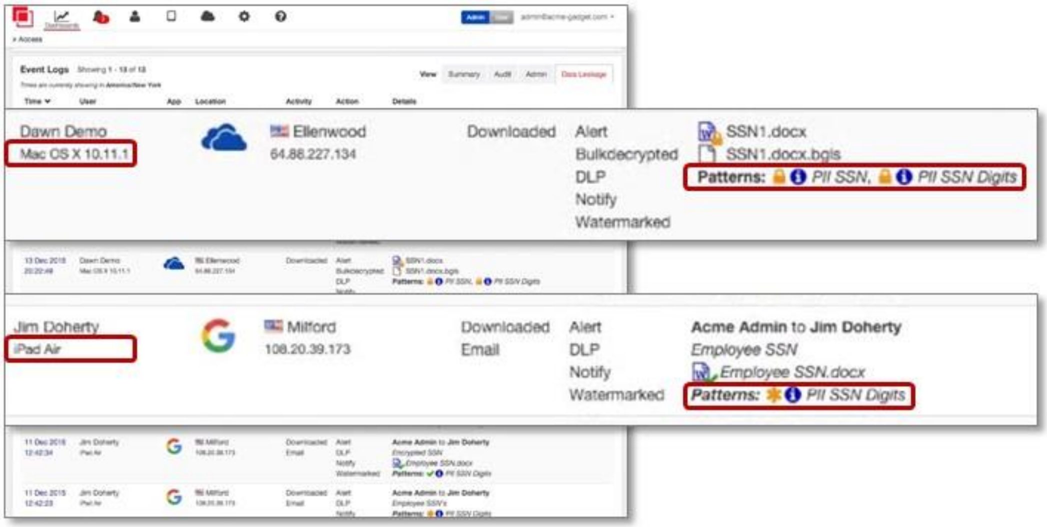
Bitglass is a Cloud Access Security Broker that aims to provide total data protection. The Bitglass CASB solution operates in the cloud, when users access data, from any device. The Bitglass approach:

- Provides secured access from any device with contextual access control, data leakage prevention, integrated multi-factor authentication and single sign-on (SSO).
- Uses 256-bit AES encryption to secure data in the cloud while keeping it fully sortable and searchable.
- Secures data on mobile devices and unmanaged BYOD systems without the need for agents or certificate installation.
- Detects anonymizers, malware hosts, command and control (C&C) servers, phishing attacks, and “shadow IT” activities.


https://portal.bitglass.com/portal/
ACME
Admin User admin@acme-gadget.com
Welcome to the Acme Gadget Portal, powered by Bitglass!
SSO
Google Apps
SSO
box
EVERNOTE
CONCUR
SSO
Dropbox
servicenow
Feedback Terms of Use Privacy Policy

With Bitglass, users interact with virtually any cloud or on-premises application, including office suites like Google Apps or Office 365, customer relationship management software like Salesforce, and file sync and share services like Box. As users connect to their applications, they are transparently redirected through a proxy, which controls access, uploads, and downloads. This makes onboarding especially easy, since the users’ credentials will always direct them through the proxy, no matter where they connect from and on any device. An API connector connects to the app and controls data-at-rest in the cloud.

ESG Lab looked at two aspects of the Bitglass CASB solution: securing access to data from any device and securing data-at-rest on devices and in the cloud. Each time data is accessed, a complete evaluation of policies occurs and appropriate controls are applied based on the permissions of the user, the attributes of the data, and the device accessing it. Organizations can use this functionality to allow access from a variety of risk contexts, while mitigating that risk with additional data-centric controls.


Admin User admin@acme-gadget.com
Dashboards
> Access
View Summary Audit Admin Data Leakage

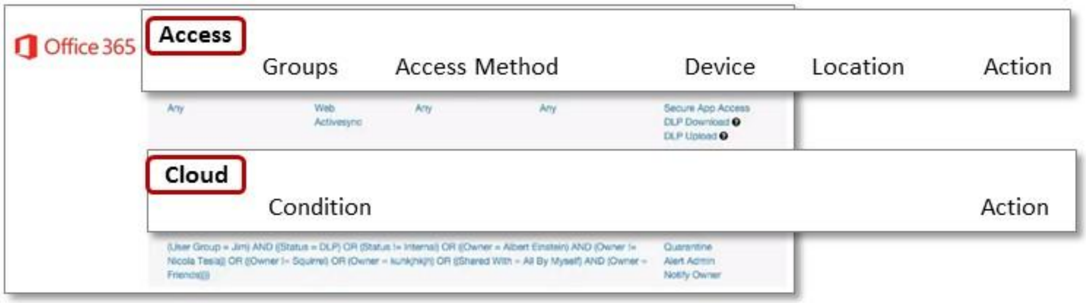
Event Logs Showing 1 - 18 of 18

Time	User	App	Location	Activity	Action	Details
	Dawn Demo Mac OS X 10.11.1		Ellenwood 64.86.227.134	Downloaded	Alert Bulkdecrypted DLP Notify Watermarked	SSN1.docx SSN1.docx.bgls Patterns: PII SSN, PII SSN Digits
	Jim Doherty iPad Air		Milford 108.20.39.173	Downloaded Email	Alert DLP Notify Watermarked	Acme Admin to Jim Doherty Employee SSN Employee SSN.docx Patterns: PII SSN Digits

In this example, two files with similar contents, social security numbers, are being accessed by two different users: one using a managed, company-issued laptop and the other using a personal iPad. The file being downloaded to the corporate laptop triggers several actions: prior to download, the file is watermarked and encrypted, and admins are alerted to a possible data loss event. When a similar file is accessed over Gmail by a user on her personal iPad, the file is watermarked and admins are alerted, but the social security numbers are redacted before the file is downloaded.

ESG Lab next looked at one of the policies that protect data on access and data at rest. For each application, access and cloud policies are completely customizable and enable organizations to flexibly define access rules appropriate for their users, their data, their device types, and their access patterns, across multiple applications.

As seen here, access to applications and the data associated with them—no matter how complex the application—can be centrally controlled with just two policies. The "Access" policy allows administrators to control access by group, method, device, or location and define multiple actions. The "Cloud" policy is focused on protection of data-at-rest and allows for the creation of a set of rules for each application to ensure that data is only stored on devices that are approved and authorized. The rule builder provides a simple and straightforward method for creating policies using prebuilt and custom rules. Bitglass can quarantine files when policies are violated, holding them until an administrator can take action.

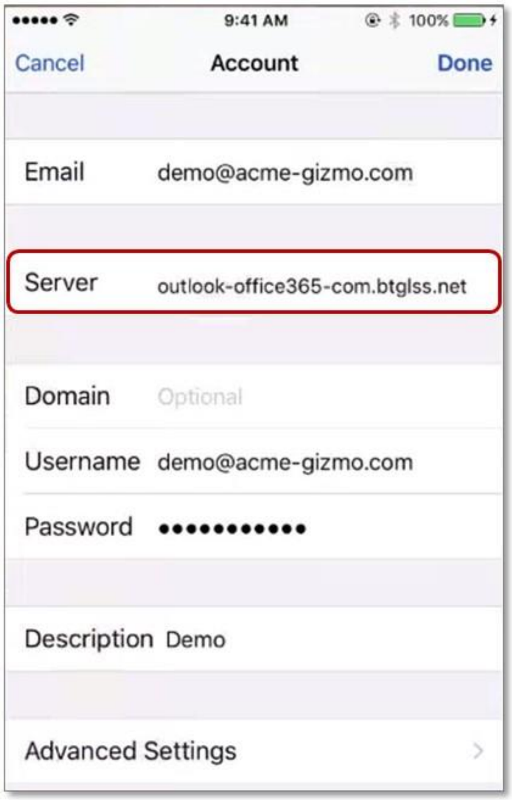


Access

Groups	Access Method	Device	Location	Action
Any	Web Activesync	Any	Any	Secure App Access DLP Download DLP Upload

Cloud

Condition	Action
(User Group = Jim) AND ((Status = DLP) OR (Status != Internal) OR ((Owner = Albert Einstein) AND (Owner != Nicola Tesla)) OR ((Owner != Squirrel) OR (Owner = kunkjnkjn) OR ((Shared With = All By Myself) AND (Owner = Friends)))	Quarantine Alert Admin Notify Owner



Cancel Account Done

Email demo@acme-gizmo.com

Server outlook-office365-com.btglss.net

Domain Optional

Username demo@acme-gizmo.com

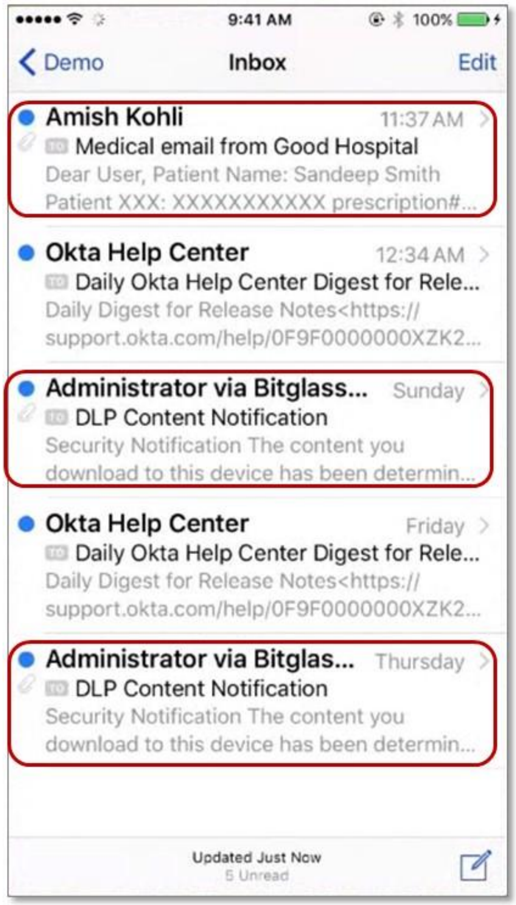
Password ••••••••••••

Description Demo

Advanced Settings

Next, ESG Lab looked at the onboarding process for an unmanaged device. In this case, a remote user is accessing email through Office365 from his iPhone. As seen here, all the user has to do is select Exchange and enter his login credentials. His data is automatically redirected through the Bitglass proxy and he will only receive authorized emails.

In this example, the user has received a number of emails that have triggered actions. The message at the top contains confidential patient data that has been redacted by Bitglass, and the two messages below have triggered DLP notifications, telling the user that the downloaded data contains sensitive information and the organization's IT department may block the download of this content in the future. Finally, ESG Lab looked at remote wipe functionality. When users are permitted to work with unmanaged BYOD devices or public cloud applications, the ability to remotely delete data or completely wipe devices is essential.



Demo Inbox Edit

Amish Kohli 11:37 AM
Medical email from Good Hospital
Dear User, Patient Name: Sandeep Smith
Patient XXX: XXXXXXXXXX prescription#...

Okta Help Center 12:34 AM
Daily Okta Help Center Digest for Rele...
Daily Digest for Release Notes<https://
support.okta.com/help/0F9F0000000XZK2...

Administrator via Bitglass... Sunday
DLP Content Notification
Security Notification The content you
download to this device has been determin...

Okta Help Center Friday
Daily Okta Help Center Digest for Rele...
Daily Digest for Release Notes<https://
support.okta.com/help/0F9F0000000XZK2...

Administrator via Bitglas... Thursday
DLP Content Notification
Security Notification The content you
download to this device has been determin...

Updated Just Now
5 Unread

Remote wipe was fast and simple to execute. ESG Lab selected the iPhone from the user's page in the Bitglass admin portal and clicked on the ***Wipe*** link next to the device name. The option to selectively wipe corporate data was selected in the pop-up window, and the next time the phone synced with the corporate email service (within a few seconds), all corporate email on the phone was removed and replaced by a message telling the user that the account was blocked on that device. Organizations can also wipe the entire device and perform a factory reset, all with no agent on the device and no mobile device management software required.

The Bigger Truth

The vast majority of organizations today are either already using applications on public cloud services or planning to. Combined with the increasing use of mobile devices and BYOD for access to potentially sensitive data, this presents a unique challenge to CISOs and IT organizations, who must provide access control, data loss prevention, and threat detection across all devices inside and outside of the firewall. CASB functionality was designed to address all of these issues.

Bitglass is a Cloud Access Security Broker whose technologies are designed to operate within and outside of the network perimeter with the ambitious goal of delivering total data protection for the enterprise—in the data center, in the cloud, on mobile devices, and anywhere on the internet.

ESG Lab confirmed that Bitglass is doing just that for managed and unmanaged devices, with no agents or certificates required. In our testing, Bitglass provided protection for data-at-rest in multiple public cloud-based applications, including data loss prevention and suspicious activity alerting. ESG Lab was able to scan and identify data at rest, set up DLP patterns, and set up policies for multiple applications quickly and easily. ESG Lab also looked at mobile access security—onboarding, securing access to and storage of data that users sync to their devices, and remotely wiping a device in seconds.

In ESG Lab's opinion, Bitglass provides a comprehensive CASB solution for an impressively large list of applications. Bitglass also protects mobile data at least as well as traditional mobile device management applications without using on-device software or agents. If your organization is currently using or planning to use public cloud applications with or without BYOD and mobile access, ESG Lab recommends taking a close look at Bitglass.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.